FAA-E-2911
03/26/98

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

National Airspace System (NAS)

System Level Specification

National Airspace System (NAS)

Infrastructure Management System (NIMS)

Managed Subsystems

FOREWORD

This document provides generic National Airspace System (NAS) Infrastructure Management System (NIMS) functional requirements and verification methods for NAS subsystems. Applicable NIMS requirements and test methods should be selected from this document for integration into the subsystem functional requirements specification.

This specification should not be invoked on a blanket basis, since some requirements may not apply to a given subsystem. At the time of inception of the subsystem specification, the subsystem Integrated Product Team (IPT), the Infrastructure IPT, Systems Engineering, Air Traffic (AT), and appropriate Airway Facilities (AF) organizations, will determine the set of requirements that will apply to the subsystem. Since it is the intention to use commercial off-the-shelf (COTS) capabilities to satisfy these requirements whenever possible, the final application of these requirements will not be determined until the COTS management capabilities can be determined. Once the final application is determined, the vendor will develop a subsystem specific interface control document for approval by the Federal Aviation Administration (FAA).

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Paragraph Title Page

LIST OF FIGURES

LIST OF TABLES

1. SCOPE

This specification establishes functional and performance requirements for subsystems which will be managed by the National Airspace System (NAS) Infrastructure Management System (NIMS). This specification is to be used in conjunction with Federal Aviation Administration (FAA) standards profiles and protocol specific implementation guidance to establish procurement requirements for NIMS managed subsystems. References to applicable standards profiles are supplied in FAA-HDBK-002. General requirements for interfacing to NIMS managed subsystems are supplied in the NIMS Manager/Managed Subsystem Interface Requirements Document (NAS-IR-51070000). Detailed requirements for interfacing to NIMS managed subsystems are supplied in the NIMS Manager/Managed Subsystem using the Simple Network Management Protocol Version 1 (SNMPv1) Interface Control Document (NAS-IC-51070000-1).

1.1 System overview.

The purpose of the NIMS is to provide automation support services for the management of the NAS infrastructure. The NIMS is based on the conceptual model of open systems management defined in the Open System Interconnection (OSI) Basic Reference Model - Part 4, Management Framework: ISO 7498-4 and OSI System Management Overview: ISO 10040. According to this model, management activities are accomplished by the interaction of applications, which operate in either the role of a manager or an agent. A manager has responsibility for one or more management activities, while an agent is responsible for managing the resources within its local system environment. An agent performs management operations on local resources as directed by a manager and forwards management related notifications, which are emitted by its local resources. As illustrated in Figure 1-1, a managed subsystem may be a NAS subsystem with an embedded agent function or a NAS subsystem which uses an external proxy agent to convert a proprietary or otherwise non-NIMS interface to a NIMS accepted protocol. This specification defines the agent capabilities to be provided by NIMS managed subsystems. The agent function is assumed to include instrumentation of the managed subsystem as required. See Section 6.3 for more detailed information.

1.2 Document overview.

The remainder of this specification presents the following information:

a) Section 2 lists government and non-government documents applicable to this specification. It includes requirements documents that form a part of this specification.

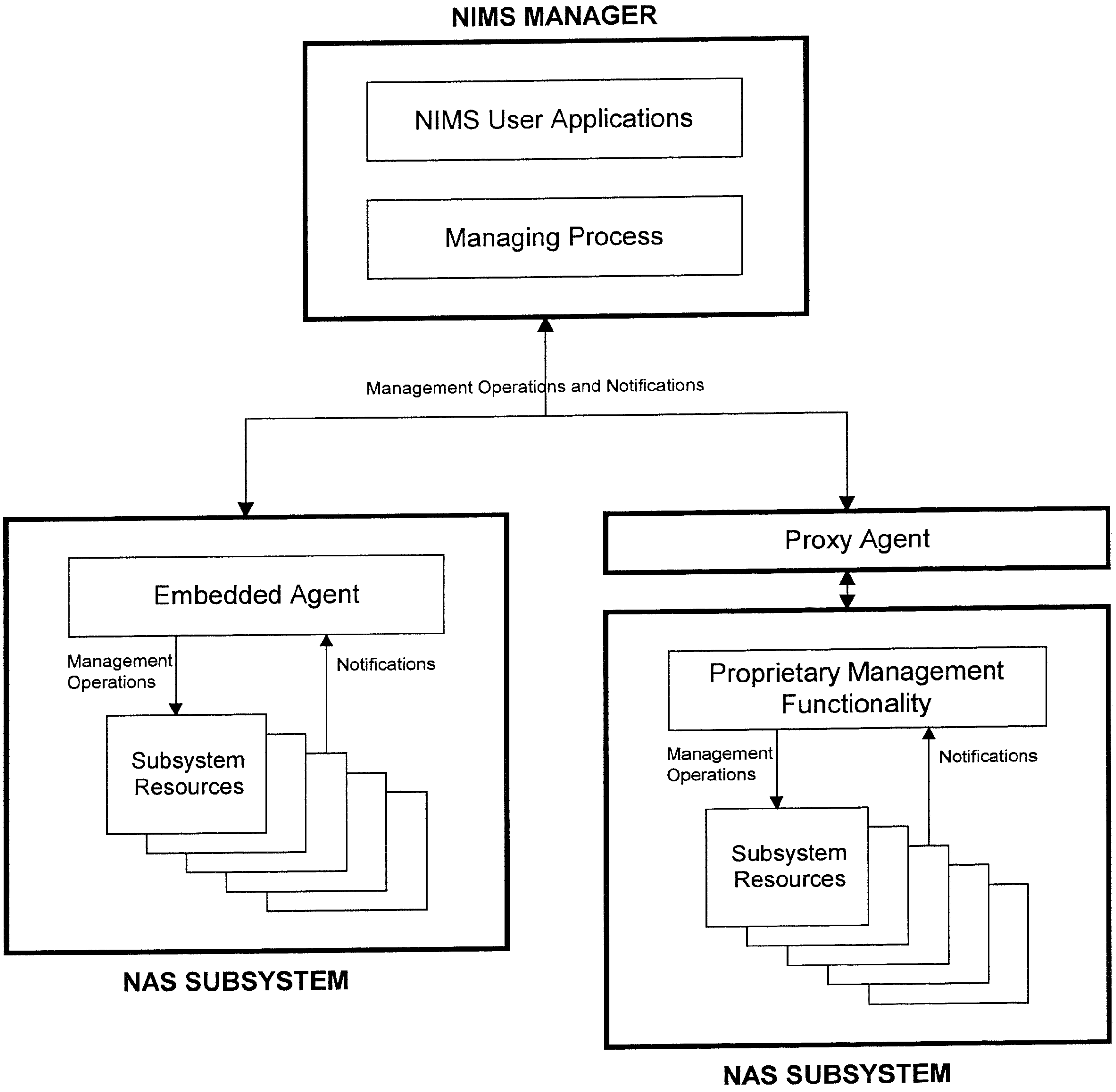

Figure 1-1. NIMS Manager to Managed Subsystem Relationship

b) Section 3 specifies NIMS requirements for managed subsystems which include:

- Functional requirements (3.1)
- System capabilities requirements(3.2)
- System external interface requirements (3.3) - NAS subsystem specific[1]
- System internal interface requirements (3.4)
- System internal data requirements (3.5)
- Adaptation requirements (3.6) - NAS subsystem specific
- Safety requirements (3.7) - NAS subsystem specific
- Security and privacy information (3.8)
- Other requirements (3.9 - 3.17) NAS subsystem specific

c) Section 4 identifies quality assurance requirements.

d) Section 5 includes the verification traceability matrix.

e) Section 6 contains a glossary and list of acronyms.

[1] NAS subsystem specific requirements will be documented in the NAS subsystem system level specification.

2. APPLICABLE DOCUMENTS

This section lists the government and non-government documents, including specifications, standards, guidelines, handbooks, and other publications that apply to this specification.

2.1 Government documents.

The following documents form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be the superseding requirement.

2.1.1 FAA specifications.

NAS-IR-51070000:1997	NAS Infrastructure Management System Manager/Managed Subsystem Interface Requirements Document
NAS-IC-51070000-1:1997	NAS Infrastructure Management System Manager/Managed Subsystem using the Simple Network Management Protocol Version (SNMPv1) Interface Control Document

2.1.2 FAA standards.

FAA-HDBK002:1997	National Airspace System (NAS) Open Systems Management

2.2 Non-government documents.

2.2.1 International Organization for Standardization (ISO).

ISO 7498-4:1989	Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 4: Management Framework
ISO 8824:1987	Information Processing Systems - Open Systems Interconnection Specifications of Abstract Syntax Notation One (ASN.1)
ISO 9000-3:1993	Quality Management and Quality Assurance Standard: Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software
ISO 9001:1994	Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation, and Servicing
ISO 10040:1992	Information Technology - Open Systems Interconnection Systems Management Overview

3. REQUIREMENTS

3.1 System functional requirements.

a) The managed subsystem shall be able to monitor the status of the managed subsystem.

b) The managed subsystem shall be able to provide notification of the occurrence of events.

c) The managed subsystem shall be able to support requested management operations.

d) The state or mode of operation of the managed subsystem shall be as stated in the specific NAS subsystem specification.

3.2 System capability requirements.

3.2.1 Subsystem monitoring.

a) The managed subsystem shall monitor NAS subsystem resources for primary and backup equipment.

b) The managed subsystem shall perform monitoring on a continuing basis, concurrent with the operational mission of the managed subsystem.

c) The managed subsystem shall perform monitoring without interfering with the operational mission of the managed subsystem.

d) The managed subsystem shall perform monitoring automatically without the need for user intervention.

e) The managed subsystem shall perform automatic self-tests (for example, diagnostics, loop-back tests, etc.) as required to determine the status of the managed subsystem without interfering with the operational mission of the managed subsystem.

3.2.1.1 Data acquisition.

a) The managed subsystem shall acquire NAS subsystem resources attributes necessary to determine the fault, configuration, performance, and security status of the managed subsystem.

b) The managed subsystem shall acquire attributes of NAS subsystem resources necessary to certify the managed subsystem.

3.2.1.2 Status determination.

3.2.1.2.1 Fault status determination.

a) The managed subsystem shall determine the operating status of each hardware component of the managed subsystem to the line replaceable unit (LRU) level.

b) The managed subsystem shall determine the operating status of each software component of the managed subsystem.

c) The managed subsystem shall determine the operating status of each external subsystem interface of the managed subsystem.

d) The managed subsystem shall determine the operating status of each subsystem function of the managed subsystem.

e) The managed subsystem shall determine the operating status of the management agent process of the managed subsystem.

f) The managed subsystem shall determine the environmental status, if applicable (for example, smoke, fire, temperature, or physical intrusion attributes), of the managed subsystem.

3.2.1.2.2 Configuration status determination.

a) The managed subsystem shall determine the physical configuration of subsystem resources.

b) The managed subsystem shall determine the logical configuration of subsystem resources.

c) The managed subsystem shall determine the availability status of subsystem resources.

3.2.1.2.3 Performance status determination.

a) The managed subsystem shall determine the workload of subsystem resources using pre-established thresholds.

b) The managed subsystem shall determine the throughput and response time of subsystem resources using pre-established thresholds.

3.2.1.2.4 Security status determination.

a) The managed subsystem shall determine the security status of subsystem resources using pre-established security rules for, but not limited to, access control.

b) The managed subsystem shall log all security violations.

3.2.1.3 Data Reporting.

3.2.1.3.1 Event Reporting.

a) The managed subsystem shall report an event whenever there is a change in the fault, configuration, performance, or security status of the managed subsystem.

b) The managed subsystem shall report an event only once for each instance of that event.

c) The managed subsystem shall apply event forwarding discriminators to filter event reporting.

3.2.1.3.2 Solicited data reporting.

a) The managed subsystem shall report monitored (sensor and derived) attributes of subsystem resources upon request.

b) The managed subsystem shall report control attributes of subsystem resources upon request.

c) The managed subsystem shall report the most recently obtained attributes of subsystem resources when requested.

d) The managed subsystem shall report security logs upon request.

3.2.2 Subsystem control.

a) The managed subsystem shall provide a response to all control operations with the command results or an indication of command execution.

b) The managed subsystem shall enforce pre-established access control rules when performing a control operation.

3.2.2.1 Initiate action.

a) The managed subsystem shall provide the capability to set/reset the subsystem or subsystem resources to a known state.

b) The managed subsystem shall provide the capability to perform diagnostics in order to detect and/or isolate faults.

3.2.2.2 Modify managed resource attributes.

a) The managed subsystem shall provide the capability to adjust event forwarding discriminators.

3.2.2.2.1 Fault Management attributes.

a) The managed subsystem shall provide the capability to adjust fault management thresholds.

b) The managed subsystem shall provide the capability to adjust attributes which condition automatic fault isolation and fault recovery processing.

3.2.2.2.2 Configuration Management attributes.

a) The managed subsystem shall provide the capability to change the physical configuration of the subsystem resources.

b) The managed subsystem shall provide the capability to change the logical configuration of the subsystem resources.

c) The managed subsystem shall provide the capability to change the administrative status of subsystem resources.

3.2.2.2.3 Performance Management attributes.

a) The managed subsystem shall provide the capability to modify general control attributes of subsystem resources.

b) The managed subsystem shall provide the capability to adjust performance thresholds.

3.2.2.2.4 Security Management attributes.

a) The managed subsystem shall provide the capability to modify managed resource attributes, that determine rules for security mechanism including but not limited to access control.

3.2.2.3 Automatic fault isolation and recovery.

a) The managed subsystem shall automatically initiate fault isolation processing (e.g., diagnostics) or fault correlation processing in response to specific events, when the faulty LRU is not uniquely determined by the event condition.

b) The managed subsystem shall automatically initiate fault recovery processing (e.g., reconfiguration) when a fault has been isolated.

3.2.3 Performance characteristics.

a) The maximum processing time shall be derived using the upper limit of the 95% confidence interval of the true average processing time (assumes normal distribution with a standard deviation of 1 second).

b) The managed subsystem shall process event notifications within an average time of 2 seconds and a maximum time of 4 seconds. The processing time is measured from the time the managed subsystem determines an event to the time the managed subsystem transmits the first byte of the notification. Excluding connection establishment time.

c) The managed subsystem shall process requests for data within an average time of two seconds and a maximum time of 4 seconds. The time is measured from the time the managed subsystem receives the last byte of the data request to the time that the managed subsystem transmits the first byte of the response.

d) The managed subsystem shall process a maintenance control command within average time of 1 second and a maximum time of three seconds. The process time is measured from the time the managed subsystem receives the last byte of the control command to the time that the managed subsystem transmits the first byte of the response or acknowledgment.

3.3 System external interface requirements.

Non-NIMS interfaces shall be in accordance with the specific NAS subsystem specification.

3.4 System internal interface requirements.

a) The managed subsystem interface shall be in accordance with the NIMS Manager/Managed Subsystem Interface Requirements Document (NAS-IR-51070000).

b) The managed subsystems using non-compliant interfaces shall be equipped with a proxy agent.

c) The managed subsystem shall be capable of providing dial-up connectivity.

d) The managed subsystem shall apply data-origin authentication procedures when dial-up connections are employed.

3.5 System internal data requirements.

a) Identifiable subsystem resources shall be organized in a management information base (MIB).

b) The managed subsystem shall organize attributes in MIB to correspond to identifiable subsystem resources.

c) The managed subsystem MIB shall be created in a medium and according to a syntax, for example, Abstract Syntax Notation One (ASN.1), that can be used by the managing system.

3.6 Adaptation requirements.

The adaptation requirements shall be in accordance with the specific NAS subsystem specification.

3.7 Safety requirements.

The safety requirements shall be in accordance with the specific NAS subsystem specification.

3.8 Security and privacy requirements.

The managed subsystem shall enforce pre-established access control rules when processing all maintenance control commands.

3.9 System environment requirements.

The system environmental requirements shall be in accordance with the specific NAS subsystem specification.

3.10 Computer resource requirements.

The computer resource requirements shall be in accordance with the specific NAS subsystem specification.

3.11 System quality factors.

The system quality factors shall be in accordance with the specific NAS subsystem specification.

3.12 Design and construction constraints.

The design and construction constraints shall be in accordance with the specific NAS subsystem specification.

3.13 Personnel related requirements.

The personnel related requirements shall be in accordance with the specific NAS subsystem specification.

3.14 Training-related requirements.

The training related requirements shall be in accordance with the specific NAS subsystem specification.

3.15 Logistic-related requirements.

The logistic related requirements shall be in accordance with the specific NAS subsystem specification.

3.16 Other requirements.

All other requirements shall be in accordance with the specific NAS subsystem specification.

4. QUALITY ASSURANCE

4.1 ISO standards.

The managed system shall comply with Quality Assurance (QA) provision as defined in Quality Management and Quality Assurance Standards: ISO 9001 and ISO 9000-3.

4.2 Completeness.

The quality assurance provisions shall also ensure that the methods of design and development are complete, that design risks are minimized, and that all developed hardware, software, and documentation meet specified requirements.

4.3 Detection of deficiencies.

The quality assurance provisions shall also ensure that the methods of design, construction, inspection, and testing provide early detection of deficiencies and assure prompt, effective corrective action.

5. VERIFICATION

5.1 General.

Verification requirements shall be in accordance with Table 5-1, Verification Requirements Traceability Matrix (VRTM). The verification levels and methods are given in paragraph 5.3.

5.2 Special verification requirements.

There are no special verification requirements imposed by this specification.

5.3 Verification levels and methods.

The following subparagraphs list and define the levels and methods of verification appropriate for use in the VRTM given in Table 5-1 of this specification.

5.4 Verification levels.

There are three basic levels of verification. All requirements imposed by Section 3 of the specification shall be verified at one or more of the following three levels:

a. Subsystem level. This level of verification is usually accomplished at the contractor's facility and culminates in the formal acceptance of the contractual end-item.

b. Integration level. This level of verification is conducted at the FAA specified test facility. The verification will determine if the system to be deployed for site installation will perform in the NAS environment and in accordance with NAS System level operational functional requirements.

c. Site level. This level of verification is usually performed at the designated site. The verification portion of the subsystem installation and checkouts will emphasize the demonstration of the overall system performance requirements. It includes the demonstration of an end-item, subsystem and or system, the final acceptance demonstration, and commissioning activities. All verification levels for subsystem to facility interfaces would normally occur at the installation site.

5.5 Verification methods.

a. Test. Test is a method of verification wherein performance is measured during or after the controlled application of functional and/or environmental stimuli. Quantitative measurements are analyzed to determine the degree of compliance. The process uses standardized laboratory equipment, procedures, hardware, and/or services.

b. Demonstration. Demonstration is a method of verification where qualitative determination of properties is made for a configuration item, including software and/or technical data and documentation. The items being verified are observed, but not quantitatively measured.

c. Analysis. This method of verification consists of comparing hardware or software design with known scientific and technical principles, procedures, and practices to estimate the capability of the proposed design to meet the mission and system requirements.

d. Inspection. Inspection is a method of verification to determine compliance without the use of special laboratory appliances, procedures, or services, and consists of a non-destructive static-state examination of the hardware, software, and/or the technical data and documentation.

Table 5-1. Verification Requirements Traceability Matrix (Verification methods: D Demonstration, I - Inspection, A - Analysis, T - Test, X - Not Applicable)

Section	Requirement	Subsys tem Level	Integra-tion Level	Site Level	Remarks
3.	REQUIREMENTS				Title
3.1	System functionality				Title
3.1.a	Monitor status	D	D	D	
3.1.b	Notification of event occurrences	D	D	D	
3.1.c	Support management operations	D	D	D	
3.2	System capability requirements				Title
3.2.1	Subsystem monitoring				Title
3.2.1.a	Monitor resources for primary and backup equipment	D	D	D	
3.2.1.b	Monitor on continuing basis	D	D	X	
3.2.1.c	Monitor without interfering with subsystem operational mission	D	D	X	
3.2.1.d	Monitor without operator intervention	D	D	X	
3.2.1.e	Perform automatic self-tests	D	D	X	
3.2.1.1	Data acquisition				Title
3.2.1.1.a	Acquire attributes to determine fault, configuration, performance, and security status	D	D	D	

Section	Requirement	Subsys tem Level	Integra-tion Level	Site Level	Remarks
3.2.1.1.b	Acquire attributes for certifying managed subsystem	D	D	D	
3.2.1.2	Status determination				Title
3.2.1.2.1	Fault status determination				Title
3.2.1.2.1.a	Determine the operating status of each hardware component	D	D	D	
3.2.1.2.1.b	Determine the operating status of each software component	D	D	D	
3.2.1.2.1.c	Determine the operating status of each external interface	D	D	D	
3.2.1.2.1.d	Monitor attributes to determine the operating status of each function	D	D	D	
3.2.1.2.1.e	Determine the operating status of the agent process	D	D	X	
3.2.1.2.1.f	Determine the environmental status of the managed subsystem	D	D	D	
3.2.1.2.2	Configuration determination				Title
3.2.1.2.2.a	Determine the physical configuration of subsystem resources	D	D	X	
3.2.1.2.2.b	Determine the logical configuration of subsystem resources	D	D	X	
3.2.1.2.2.c	Determine the administrative status of subsystem resources	D	D	D	
3.2.1.2.3	Performance status determination				Title
3.2.1.2.3.a	Determine the workload of subsystem resources	D	D	X	
3.2.1.2.3.b	Determine throughput and response time of subsystem resources	D	D	X	
3.2.1.2.4	Security status determination				Title
3.2.1.2.4.a	Determine the security status of subsystem resources	D	D	D	
3.2.1.2.4.b	Log all access rule violations	D	D	X	
3.2.1.3	Data reporting				Title
3.2.1.3.1	Event reporting				Title
3.2.1.3.1.a	Report changes in fault, configuration, performance, or security status	D	D	D	
3.2.1.3.1.b	Report event only once	D	D	X	
3.2.1.3.1.c	Apply event forwarding discriminators	D	D	X	
3.2.1.3.2	Solicited data reporting				Title
3.2.1.3.2.a	Report monitored attributes	D	D	X	

Section	Requirement	Subsystem Level	Integration Level	Site Level	Remarks
3.2.1.3.2.b	Report control attributes	D	D	X	
3.2.1.3.2.c	Report most recently obtained attributes	D	D	X	
3.2.1.3.2.d	Report security logs	D	D	X	
3.2.2	Subsystem control				Title
3.2.2.a	Provide response to all control operations	D	D	D	
3.2.2.b	Enforce pre-established access control rules	D	D	D	
3.2.2.1	Initiate action				Title
3.2.2.1.a	Provide capability to (re)-set resource to know state	D	D	D	
3.2.2.1.b	Provide capability to perform diagnostics	D	D	X	
3.2.2.2	Modify managed resource attributes				Title
3.2.2.2a	Provide event forwarding discriminator adjustment control	D	D	X	
3.2.2.2.1	Fault Management Attributes				Title
3.2.2.2.1.a	Provide fault management threshold adjustment control	D	D	X	
3.2.2.2.1.b	Provide control of automatic fault isolation and fault recovery processing	D	D	X	
3.2.2.2.2	Configuration management attributes				Title
3.2.2.2.2.a	Provide physical configuration change control	D	D	X	
3.2.2.2.2.b	Provide logical configuration change control	D	D	X	
3.2.2.2.2.c	Process administrative state change maintenance control command	D	D	D	
3.2.2.2.3	Performance management attributes				Title
3.2.2.2.3.a	Provide performance attribute control	D	D	X	
3.2.2.2.3.b	Provide performance threshold adjustment control	D	D	X	
3.2.2.2.4	Security management attributes				Title
3.2.2.2.4.a	Provide control for modification of access control rules	D	D	X	
3.2.2.3	Automatic fault isolation and recovery				Title
3.2.2.3.a	Automatically initiate fault isolation processing	D	D	X	
3.2.2.3.b	Automatically initiate fault recovery processing	D	D	X	
3.2.3	Performance characteristics				Title
3.2.3.a	Maximum processing time	D	X	X	
3.2.3.b	Process events within average of 2	T	T	X	

Section	Requirement	Subsystem Level	Integration Level	Site Level	Remarks
	seconds and maximum of 4 seconds				
3.2.3.c	Process requests within average of 2 seconds and maximum of 4 seconds	T	T	X	
3.2.3.d	Process commands within average of 2 seconds and maximum of 3 seconds	T	T	X	
3.3	System external interface requirements	X	X	X	Title
3.4	System internal interface requirements				Title
3.4a	In accordance with NAS-IR-51070000	D	X	X	
3.4.b	Non-compliant interfaces equipped with proxy agents	I	X	X	
3.4.c	Capable of providing dial-up connectivity	D	D	X	
3.4.d	Apply data-origin authentication procedures to dial-up connections	D	D	X	
3.5	System internal data requirements				Title
3.5.a	Identifiable subsystem resources organized in a management information base (MIB)	I	X	X	
3.5b	Organize attributes in MIB to correspond to identifiable subsystem resources	I	X	X	
3.5.c	Create MIB in medium and syntax that can be used by managing system	I	X	X	

6. NOTES

6.1 Glossary.

Access Control Rule - Access control rules specify the criteria to be met in order to grant or deny users (initiators) access to subsystem resources (targets).

Administrative State – An attribute, which indicates whether or not a managed resource is "available" or "not available" to provide its intended service. This state is set by the NIMS Manager to effect or reflect the status of the managed resource.

Availability Status - A monitored attribute that provides more specific information on the condition of the managed resource allocated to provide service. The availability status for the "available" and "not available" administrative states include the following:

Available

- On-line
- Power on

Not Available

- Off-line
- Power on
- Maintenance
- Failed

Agent - The agent refers to that subsystem function that performs remote monitoring and effects control for the purpose of system management.

Attribute - Each managed resource will have one or more attributes. Attributes are characteristics or parameters of managed resources. In the context of monitoring, attribute refers to sensor or derived data that is directly obtained during data acquisition or determined by status determination processing. In the context of control, attribute refers to effectors or actuators that are subject to adjustment via control commands.

Certification - Certification is the process of determining the quality of the required or advertised services being provided to the user of the systems, subsystems, and equipment.

Configuration - Data describing how subsystem resources are physically or logically structured for operation. The physical configuration of subsystem resources refers to the structure of hardware entities, which are managed. This structure is typically beyond the LRU level; for example, the physical configuration may indicate which ports on an interface card are configured on a site-specific basis. The logical structure of subsystem resources refers to the structure of software or functional entities such as virtual circuits on a communication subsystem.

Configuration Management - Configuration management facilities allow system managers to exercise control over the configuration of the managed subsystem, change the administrative state of subsystem resources, and control the reporting of events emitted by subsystem resources.

Data-Origin Authentication - Data-origin authentication procedures insure that the origin of transmitted data is as claimed.

Degraded - The managed resource is not operating in the ideal range but operating within an acceptable range.

Derived Data - Derived data refers to monitored data that is determined from an interpretation of other sensor data (or recursively other derived data) or that is provided by a computing device (for example, self-test results from diagnostic equipment).

Event Forwarding Discriminator - Event forwarding discriminators are attributes that are used to determine which event reports are to be forwarded to particular destinations. The discriminators operate on potential event reports initiated during status determination and condition when a real event report is to be generated. Simple discriminators may be used to merely enable or disable reporting of specific events. More sophisticated discriminators may be time based and filter event reporting for specific time intervals.

External Subsystem Interface - An external subsystem interface is a managed subsystem resource. It is an identifiable component for which operating status must be determined. The operating status for an external subsystem interface indicates the ability to communicate with other subsystems.

Failed - The managed resource is operating outside the acceptable operating range.

Fault Management - Fault management facilities allow system managers to manage problems and include mechanisms for the detection, isolation and correction of abnormal system operation.

Fault Thresholds - Fault thresholds are control attributes associated with the operating range of a resource. Fault thresholds are used to determine when there is a change in the operating status of a resource. A fault threshold may be an absolute count, a fixed or sliding window count interval, a value and duration, or an absolute value.

Function - A function is a managed subsystem resource. A function in a managed subsystem is a specific capability, which the subsystem provides. A function contributes to a NAS service since the functions of one or more subsystems combine to provide a system service to NAS users.

Hardware Component - A hardware component is a subsystem resource that is a discrete subsystem physical entity. It may be comprised of one or more LRUs.

Line Replaceable Unit (LRU) - An LRU is the lowest possible unit to be replaced within the subsystem during site level maintenance activities. It is a separate, installable physical package performing a single function or groups of closely related functions.

Maintenance Control Commands - Maintenance control commands provide for manual control of a subsystem for management purposes. Generic maintenance control commands represent a minimal control capability for management operations.

Managed resources - resources that may be managed through the use of management protocols.

Normal - The managed resource is operating within the ideal operating.

Operating Status - Operating status is a monitored attribute, which indicates to the extent to which a subsystem resource can perform its intended operation. Operating status is resource dependent and the specific characterization varies with the operating range of the resource. Four indicators are provided to characterize the operational status of a resource: normal, warning, degraded, and failed.

Performance Management - Performance management facilities provide the system manager with the ability to monitor and evaluate the performance of the subsystem.

Performance Thresholds - Performance thresholds are resource attributes, which control events associated with resource workload monitoring and function throughput and response times.

Proxy agent – entity capable of providing interface conversion with a non-standard agent, to perform management operations on managed objects and emits notification on behalf of managed objects.

Security Management - Security management facilities allow a system manager to manage those services that provide access protection of system resources.

Sensor Data - Sensor data refers to the analog or discrete data that is obtained from a device for monitoring purposes. Analog sensor data must generally be converted to digital form and sometimes be conditioned prior to examination for status determination.

Software Component - A software component is subsystem resource that is a distinctly identifiable segment of software. A software component has discrete functionality, and can be separately monitored and, optionally, controlled.

Subsystem Control - Subsystem control includes the external control capability of a managed subsystem, and automatic fault isolation and recovery processing. External control is initiated by the managing system to affect or alter the managed subsystem. Automatic fault isolation and recovery operations are initiated by the managed subsystems without external intervention.

Subsystem Monitoring - Subsystem monitoring is the acquisition of managed resource attributes, examination of these attributes to determine status, and the automatic and solicited reporting of acquired data and status information.

Subsystem Operating Status - Subsystem operating status is an attribute that indicates the extent to which a monitored subsystem can perform all of its intended subsystem functions, and as such is derived directly from the operating status of each of the subsystem functions.

System Management Functional Area (SMFA) - ISO 7498-4 describes sets of management facilities called system management functional areas. SMFAs are the major work areas or tasks of systems management. Five system management functional areas have been defined in ISO: Fault Management, Configuration Management, Performance Management, Security Management, and Accounting Management

Warning - The managed resource is still capable of performing all of its functions at the ideal level of performance, but some aspect to the resource has changed such that management action is required.

6.2 Acronyms.

AF	Airway Facilities
ASN.1	Abstract Syntax Notation One
AT	Air Traffic
COTS	Commercial Off The Shelf
FAA	Federal Aviation Administration
IPT	Integrated Product Team
IR	Interface Requirements
ISO	International Organization for Standardization
LRU	Line Replaceable Unit
MIB	Management Information Base
NAS	National Airspace System
NIMS	NAS Infrastructure Management System
OSI	Open Systems Interconnection
PT	Product Team
SNMP	Simple Network Management Protocol
VRTM	Verification Requirements Tractability Matrix

6.3 System overview.

The purpose of the NIMS is to provide automation support services for the management of the NAS infrastructure. The NIMS is based on the conceptual model of open systems management defined in the Open System Interconnection (OSI) Basic Reference Model - Part 4, Management Framework: ISO 7498-4 and OSI System Management Overview: ISO 10040. According to this model, management activities are accomplished by the interaction of applications, which operate in either the role of a manager or an agent. A manager has responsibility for one or more management activities, while an agent is responsible for managing the resources within its local system environment. An agent performs management operations on local resources as directed by a manager and forwards management related notifications, which are emitted by its local resources.

6.3.1 Resource categories.

In general, any NAS subsystem may be viewed in terms of its components (what it consists of), in terms of its functions (what it does), or as a single entity. This specification categorizes the resources of a managed subsystem at a first level according to these three distinct aspects of the subsystem.

The distinct entities that comprise a managed subsystem are termed subsystem components. For the purpose of this requirement specification, subsystem components are further classed into three general types of components: hardware, software, and external interface components. A hardware component is an identifiable subsystem resource that is a discrete physical entity. This specification requires that managed subsystems determine the operating status of hardware components to the line replaceable unit (LRU). A second general component type is a software component. A software component is a subsystem resource that is a distinctly identifiable segment of the subsystem software. A software component has discrete functionality that can be separately monitored and controlled. The third general type of component is an external interface. Since managed subsystems are generally connected to other subsystems in the NAS, it is important that the external interfaces be managed as distinct resources. It should be noted that an external interface component might be a logical entity such as a switched virtual circuit or a transport connection.

A function in a managed subsystem is a specific capability which the subsystem provides and which contributes to a NAS service in the sense that the functions of one or more subsystems combine to provide a system service to NAS users. The components and functions of a subsystem are related inasmuch as a given function that a subsystem performs is necessarily dependent on the components which are involved in providing that function.

The view of a subsystem as a single entity is necessary to support management of the NAS at a service level, where it is useful to have a summary view of the operating status of each of the subsystems which combine to provide NAS services.

6.3.2 Resource attributes.

Management actions on subsystem resources involve monitoring and control of specific resource characteristics or parameters. In this specification, resource characteristics or parameters are termed attributes. There are two classes of attributes: monitor attributes and control attributes. Monitor attributes are the sensor or derived data of a resource, which are directly acquired or indirectly determined during acquisition and status determination processing. Control attributes are the effectors or actuators that are subject to adjustment by control operations.

6.4 Functional Requirements Partitioning

The functional requirements for a NIMS managed subsystem are specified by the "shall" statements contained in Section 3. This section describes the partitioning of requirements in general. and the following subsections present summary descriptions of each function to provide the general context of Section 3 requirements.

At a first level, functional requirements have been grouped into two major categories: subsystem monitoring and subsystem control.

Subsystem monitoring entails the active acquisition of managed resource attributes, examination of these attributes to determine status at various levels, and automatic reporting of status information. Subsystem monitoring also includes reporting of management information on a request-response basis.

Subsystem control in a managed subsystem refers to those capabilities required to carry out real-time or pre-determined management actions. External control commands provide the capability to alter a subsystem for the purpose of proactive or reactive management. Subsystem control functions also provide for automatic reactions to changing subsystem conditions; specifically, subsystem-initiated fault isolation and recovery actions are provided.

Where applicable and to the extent that they are distinct functions, the subsystem monitoring and control requirements specified herein are partitioned according to the system management functional areas (see glossary) that they support. The management functional areas applicable to NIMS managed subsystems are fault management, configuration management, performance management, and security management. Figure 6-1 depicts this organization.

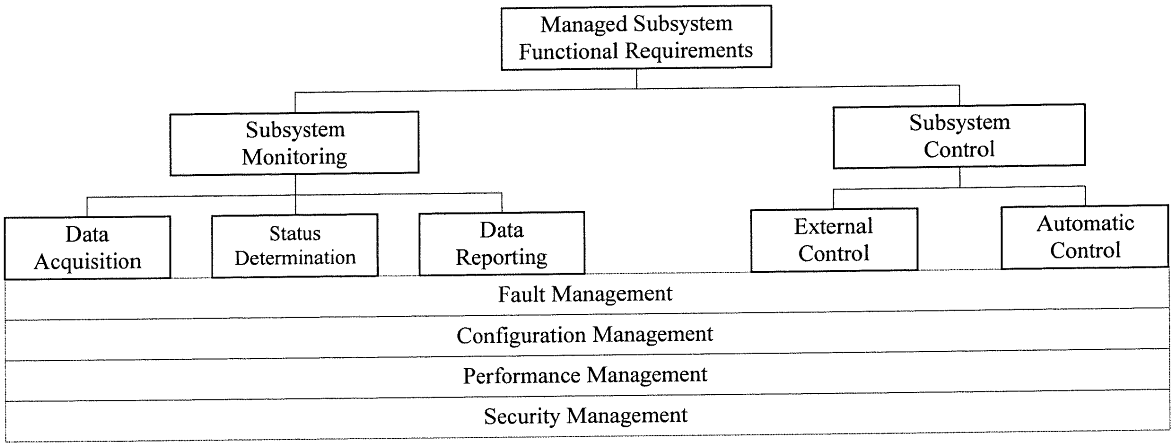

Figure 6-1. Organization of Managed Subsystem Functional Requirements

6.4.1 Subsystem monitoring.

As indicated in Figure 6-1, the requirements for subsystem monitoring is composed of three functional components; data acquisition, status determination, and data reporting. Data acquisition is a continuous process that obtains sensor and derived data attributes of subsystem resources being monitored. Once acquired, attributes are examined individually or collectively by status determination. Changes in the status of resources are reported automatically, i.e., as event notifications. In addition to automatic event reporting, data reporting provides for reporting on a request-response basis.

The managed subsystem will monitor fault, configuration, performance, and security attributes to enable the system to be managed by the NIMS manager.

6.4.1.1 Data acquisition.

Sensor and derived data necessary to determine the status of the monitored subsystems, including the agent itself, will be acquired. Data acquisition may operate by simply sampling the attributes of the subsystem resources or may involve active stimulation of the subsystem to acquire attributes that otherwise would not be obtained during normal subsystem operation. The monitored subsystem will have the sensors needed to obtain the analog, digital, and discrete signal values of its monitored resources. Stimulators will be provided for subsystems that require baseline signals to validate performance.

For developmental programs, the contractor will develop a candidate set of managed resource attributes that meet the general requirements specified herein. The NIMS Product Team (PT), with input from subject matter experts, will review the candidate set and reach an agreement with the NAS subsystem Integrated Product Team (IPT) on the approved set of resource attributes. For NAS subsystems that are non-developmental, the requirements for management information contained in this specification should not be interpreted to exclude the use of commercial off-the-shelf (COTS) products. Rather, this document should in those cases be used to evaluate candidate vendor offerings. In any case, an attribute set that collectively provides the status of the managed subsystem for each relevant management functional area will be monitored.

The fault management monitoring function involves acquisition of an attribute set from which the operating status of each subsystem resource can be derived. Operating status refers to the extent to which a subsystem resource can perform its intended operation, and in this sense, refers to the fault or failure status of a subsystem resource. By convention under NIMS, up to four distinct characterizations of a resource's operating status are possible: normal, warning, degraded, and failed (see glossary).

The configuration management monitoring function is concerned with acquisition of attributes which indicate the physical or logical configuration of subsystem resources, and attributes to derive the administrative state of selected subsystem resources. The administrative state indicates whether a subsystem resource is "available" or "not available" to provide its intended service.

The performance management monitoring function involves acquisition of attributes from which the workload of select subsystem resources can be derived, i.e., attributes which indicate the actual demand of subsystem resources. Performance monitoring will also acquire attributes to determine throughput and response time measures.

The security management monitoring function will obtain attributes required to insure the protection of subsystem resources. Subsystem resources are protected by the application of subsystem specific access control rules. Access control rules specify the criteria to be met in order to grant or deny users (initiators) access to subsystem resources (targets).

6.4.1.2 Status determination.

The managed subsystem will process acquired resource attributes to determine subsystem resource status from the perspective of each applicable management functional area.

The fault management status determination function will examine attributes of basic subsystem components. Specifically, attributes for the hardware, software, and interface components of a managed subsystem will be examined to determine their operating status. The fault status determination function will also derive the operating status of each subsystem function; i.e., the subsystem's capability to provide its intended services will be determined. From the operating status of each function, the operating status of the subsystem will be derived. The managed subsystem will perform fault correlation when necessary to derive the status of composite entities and functions. The fault status determination function will derive the operating status of resources using fault thresholds. Fault thresholds are attributes which are associated with the operating range of a resource and which determine when there is a change in the operating status of that resource. Various types of threshold attributes may be employed by managed subsystems. A threshold may simply be an absolute count, which specifies the value that a monitored counter attribute must exceed to cause a change in the operating status of a resource. More sophisticated thresholds include counts over a fixed time interval or over a sliding window consisting of value and duration controls or absolute values. In any case, an event notification will be generated if the operating status of any subsystem resource changes.

The configuration management status determination function will examine certain subsystem attributes to determine if there has been a change in the physical or logical configuration of the subsystem or if the administrative state of selected subsystem resources has changed. Such changes will be reported as event notifications.

The performance management status determination function will obtain the workload of select subsystem resources by deriving the actual demand relative to anticipated demand. An example workload measure would be the percentage utilization of on-line storage, i.e., the ratio of allocated space (actual demand) to the available storage space (anticipated demand). In addition, the performance management status determination function examines the throughput and response time measures of selected subsystem resources. As is the case with the fault status determination function, the performance status determination function uses pre-established threshold values to determine if the managed resource is operating out of range. If these values are transitioned, an event notification will be generated.

The security status determination function will generate an event whenever there is a security violation managed subsystem resources. A log of violations is also maintained.

6.4.1.3 Data reporting.

Data reporting refers to the manner in which event reporting will occur and to specific solicited reporting capabilities.

6.4.1.3.1 Event reporting.

Event reports will be sent unsolicited as a result of status determination. Events will be reported only once and as they occur. Event reporting will be controlled by the application of forwarding discriminators. Discriminators serve to filter event reports and can be used to minimize the number of reported events including events caused by transient conditions.

6.4.1.3.2 Solicited data reporting.

Upon request, the managed subsystem will report monitor or control attributes which have been obtained most recently, i.e., the most recently acquired or derived monitored attributes and control attributes which have been affected by the most recently issued command. Security logs will also be provided upon request.

6.4.2 Subsystem control.

Two functional components are distinguished under subsystem control:

a. External control,

b. Automatic fault isolation and recovery.

External control provides the capability to affect/alter a subsystem in order to perform NAS management operations. In addition to control initiated by the managing system, selected subsystems will include functions that are intended to provide an increased level of automated fault tolerance in subsystems. These functions will provide for self-diagnostics and isolation of problems and allow automatic recovery from subsystem faults.

6.4.2.1 External control.

Certain generic control capabilities are specified that represent a minimal control capability for management operations.

Whenever a control command is issued, an associated response is returned by the managed subsystem, that is, command execution is a confirmed service. The response may be the direct result of the command or in cases where command execution requires an extensive time period or is otherwise deferred, an indication of the command execution status is returned.

Fault management control functions will allow the managing system to perform fault detection, isolation, and recovery operations. The capability will be provided to adjust fault thresholds, initiate diagnostics, reset the subsystem or a subsystem resource to a known state, and control the operation of automatic processes.

Configuration management control functions will allow the managing system to modify the configuration of the managed subsystem, change the administrative state of subsystem resources, and control the reporting of events emitted by subsystem resources. Configuration management control will be used to directly support the subsystem configuration management task or to support other management functional areas. For example, configuration management control may be exercised to alleviate congestion, or to isolate or otherwise respond to fault conditions.

Performance management control functions will allow the managing system to adjust general control attributes, i.e., to conduct performance tuning activities. The managing system will also be able to adjust performance thresholds. Performance thresholds are those associated with workload monitoring, e.g., overload, and clear thresholds, as well as thresholds which govern event reporting based on throughput and response time measures.

Security management control functions will allow the managing system to modify the access control rules which are enforced whenever a maintenance control command is processed.

6.4.2.2 <u>Automatic fault isolation and recovery</u>.

Managed subsystems which provide critical NAS services will have the capability to detect, isolate, and recover from faults, without intervention by the managing system.